

REMARKS

Claims 1-21 are pending in the present application. Claims 1, 7-12, and 18-21 were rejected under 35 U.S.C. § 103(a) as allegedly being unpatentable over Roeck (U.S. Patent No. 6,594,305) in view of Nay (U.S. Patent No. 5,237,567). Claims 2-3 and 13-14 were rejected under 35 U.S.C. § 103(a) as allegedly being unpatentable over Roeck in view of Nay and further in view of Spelman (U.S. Patent No. 5,680,458). Claims 4 and 15 were rejected under 35 U.S.C. § 103(a) as allegedly being unpatentable over Roeck in view of Nay and further in view of Mergard (U.S. Patent No. 5,881,248). Claims 6 and 17 were rejected under 35 U.S.C. § 103(a) as allegedly being unpatentable over Roeck in view of Nay and further in view of Whitmire (U.S. Patent No. 6,115,817). The Examiner's rejections are respectfully traversed.

The Examiner maintains that Nay describes generating an authentication code by equating a data transfer error checking code to a security related authentication code. Applicants respectfully disagree. The Office Action indicates that Nay discovers errors in data transmission using a checksum. Even if assuming *arguendo* that the checksum of Nay equates to an authentication code, Nay still fails to signal a security violation in response to the checksum not matching the sent data. If Nay detects a problem, the data is corrected automatically using the ECC data or resent. Nay does not detect a security violation, because Nay does not contemplate that the data may be tampered with, but rather only that the data was not received properly. The Office Action asserts that a violation in Nay could be the result of tampering and, hence, the data error of Nay equates to a security violation. The Office Action fails to support this possibility based on the teachings of Nay, but rather just based on an ungrounded conclusory statement. One significant defect in this construction is that it completely ignores the effect of the “security” modifier to the violation term. As admitted by the Office Action Nay only looks

at data integrity, regardless of the source of a data error. If Nay detects an error in the sent data, the data is corrected or resent and no violation of any kind is identified, much less a security violation.

For at least the aforementioned reasons, Applicants respectfully submit that the Examiner has failed to make a *prima facie* case that the present invention is obvious over the prior art of record. Applicants request that the Examiner's rejections of claims 1-4, 6-15, and 17-21 under 35 U.S.C. 103(a) be withdrawn.

In rejecting claims 2, 3, 13, and 14 over Roeck and Nay in further view of Spelman, the Office Action suggests that it would be obvious to provide the Roeck-Nay system with out-of-band messaging to assure that the message has not been tampered with. The grounds for establishing combinability must be found in the prior art. Because Roeck and Nay are completely silent regarding identifying security violations, but rather only data transmission errors, it is inconceivable that grounds could be found in Roeck or Nay to combine Spelman therewith. Nay would have no reason to send the checksum out-of-band with respect to the data as data and checksums are conventionally always provided over the same channel. This combination constitutes an impermissible use of hindsight using Applicants' disclosure as a roadmap. For these additional reasons, claims 2, 3, 13, and 14 are themselves allowable and Applicants respectfully request the rejection of these claims be withdrawn.

In rejecting claims 4 and 15 in further view of Mergard, the Office Action suggest that it would be obvious to send the authentication code out-of-band and over an unused portion of the bus to improve bus performance. Again, Nay would have no reason to send the checksum out-of-band with respect to the data as data and checksums are conventionally always provided over the same channel. The authentication code is not sent out-of-band to improve bus performance

but rather to send the authentication code separately from the control codes to increase the difficulty that a malicious entity might have in identifying the authentication code. Again, this combination constitutes an impermissible use of hindsight using Applicants' disclosure as a roadmap. For these additional reasons, claims 4 and 15 are themselves allowable and Applicants respectfully request the rejection of these claims be withdrawn.

For the aforementioned reasons, it is respectfully submitted that all claims pending in the present application are in condition for allowance. The Examiner is invited to contact the undersigned attorney at (713) 934-4070 with any questions, comments or suggestions relating to the referenced patent application.

Respectfully submitted,

Date: July 13, 2006

/Scott F. Diring/

Scott F. Diring
Reg. No. 35,119
Williams Morgan & Amerson, P.C.
10333 Richmond Avenue, Suite 1100
Houston, TX 77042
(713) 934-4070
(713) 934-7011 (Fax)

ATTORNEY FOR APPLICANTS